

В.Н. ШЕВЧЕНКО, С.В. СИДОРОВ

О ПОДОБИИ МАТРИЦ ВТОРОГО ПОРЯДКА  
НАД КОЛЬЦОМ ЦЕЛЫХ ЧИСЕЛ

Из линейной алгебры известно (напр., [1], с. 101), что с линейным преобразованием линейного пространства  $V$  над полем  $\mathbf{F}$  связан класс  $[\varphi]$  подобных между собой матриц.  $A$  именно, этот класс состоит из всех матриц преобразования  $\varphi$  в различных базисах пространства  $V$ . Если  $A, B \in [\varphi]$ , то существует невырожденная матрица  $S$  с элементами из  $\mathbf{F}$  такая, что  $AS = SB$ . Подобие матриц  $A$  и  $B$  над полем рациональных чисел будем обозначать  $A \approx B$ . Для проверки подобия над полем  $\mathbf{Q}$  имеется алгоритм (напр., [1], с. 154–157) приведения характеристической матрицы  $A - \lambda E$  к нормальной диагональной форме Смита и построения по ней единственной канонической матрицы  $F$  (в [1], с. 181, она называется естественной нормальной формой матрицы  $A$ ).

Перенесем понятие подобия на кольцо  $\mathbf{Z}$  целых чисел. Сильно возросшие трудности заставили ограничиться двумерным случаем, в котором будет получен алгоритм проверки подобия двух матриц  $A$  и  $B$  над  $\mathbf{Z}$  и, если их характеристический многочлен приводим над  $\mathbf{Q}$ , описаны классы подобных матриц.

**Определение 1.** Будем говорить, что матрица  $B \in \mathbf{Z}^{n \times n}$  подобна матрице  $A \in \mathbf{Z}^{n \times n}$  над кольцом  $\mathbf{Z}$ , если существует  $S \in \mathbf{Z}^{n \times n}$  такая, что  $AS = SB$  и  $\det S \in \{-1, 1\}$ , и обозначать это  $A \sim B$ . При этом матрицу  $S$  будем называть  $\mathbf{Z}$ -трансформирующей  $A$  в  $B$  матрицей.

Очевидно, введенное отношение есть отношение эквивалентности.

Следовательно, множество  $\mathbf{Z}^{n \times n}$  разбивается на классы эквивалентности  $K_j$ ,  $j \in J$ . Таким образом, можно записать

$$\mathbf{Z}^{n \times n} = \bigcup_{j \in J} K_j.$$

Целочисленную матрицу  $A$  можно рассматривать как матрицу над кольцом вычетов  $\mathbf{Z}/m$ , если положить  $A = (\text{res}_m a_{ij})$ , где  $m$  — натуральное число, а  $\text{res}_m x$  — остаток от деления  $x$  на  $m$ . Обозначим через  $(\mathbf{Z}/m)^*$  множество делителей единицы в  $\mathbf{Z}/m$ .

**Определение 2.** Будем говорить, что матрица  $B \in \mathbf{Z}^{n \times n}$  подобна матрице  $A \in \mathbf{Z}^{n \times n}$  над кольцом  $\mathbf{Z}/m$ , если существует  $S \in \mathbf{Z}^{n \times n}$  такая, что  $AS \equiv SB \pmod{m}$  и  $\det S \in (\mathbf{Z}/m)^*$ , и обозначать это  $A \sim_m B$ .

Задача заключается в том, чтобы определить, являются ли две данные целочисленные матрицы  $A$  и  $B$  подобными, и если являются, то найти трансформирующую матрицу.

Над полем  $\mathbf{Q}$  критерием подобия матриц является равенство наибольших общих делителей (НОД) миноров  $k$ -го порядка их характеристических матриц. Обобщением понятия НОД на кольцо  $\mathbf{Z}[\lambda]$  является идеал, порожденный минорами  $k$ -го порядка характеристической матрицы. Так как  $\mathbf{Q}[\lambda]$  — кольцо главных идеалов, а  $\mathbf{Z}[\lambda]$  таковым не является, то это первое усложнение при переходе к  $\mathbf{Z}$ .

Работа выполнена при частичной финансовой поддержке Российского фонда фундаментальных исследований (код проекта № 05-01-00552-а).

Обозначим через  $I_k(A - \lambda E)$  идеал в кольце  $\mathbf{Z}[\lambda]$ , порожденный минорами  $k$ -го порядка характеристической матрицы  $A - \lambda E$ , а через  $\Delta_k(A)$  — НОД (рассматриваемый над кольцом целых чисел  $\mathbf{Z}$ ) миноров  $k$ -го порядка матрицы  $A$ .

**Теорема 1.** Если  $A \sim B$ , то

- 1)  $A \approx B$ ,
- 2)  $A \sim_m B$  над кольцом  $\mathbf{Z}/m$  для всех  $m \geq 2$ ,
- 3)  $I_k(A - \lambda E) = I_k(B - \lambda E)$  для всех  $k = 1, \dots, n$ ,
- 4)  $\Delta_k(A) = \Delta_k(B)$ ,  $k = 1, \dots, n$ .

**Доказательство.** Так как  $A \sim B$ , то существует матрица  $T \in \mathbf{Z}^{n \times n}$  такая, что  $\det T \in \{-1, 1\}$  и  $AT = TB$ .

- 1) Очевидно,  $T$  удовлетворяет условиям подобия над полем  $\mathbf{Q}$ .
- 2) Очевидно,  $AT \equiv TB \pmod{m}$  и  $\det T \in (\mathbf{Z}/m)^*$ , т. е.  $A \sim_m B$ .
- 3)  $(A - \lambda E)T = T(B - \lambda E)$ , откуда  $A - \lambda E = T(B - \lambda E)T^{-1}$ . Из формулы Бине–Коши (напр., [2], с. 19) следует, что любой минор  $k$ -го порядка матрицы  $A - \lambda E$  принадлежит  $I_k(B - \lambda E)$ . Следовательно,  $I_k(A - \lambda E) \subseteq I_k(B - \lambda E)$ . Аналогично доказывается обратное включение.
- 4) Доказательство проводится аналогично предыдущему пункту теоремы.  $\square$

Заметим, что условие 1) является следствием условия 3).

**Теорема 2.** Пусть  $A, B \in \mathbf{Z}^{n \times n}$ ,  $A \sim_m B$  и  $A \sim_k B$ , где  $m$  и  $k$  — взаимно простые числа. Тогда  $A \sim_{mk} B$ .

**Доказательство.** Существуют матрицы  $T = (t_{ij}) \in (\mathbf{Z}/m)^{n \times n}$ ,  $S = (s_{ij}) \in (\mathbf{Z}/k)^{n \times n}$  такие, что

$$AT \equiv TB \pmod{m}, \quad AS \equiv SB \pmod{k} \quad (1)$$

и  $\det T \in (\mathbf{Z}/m)^*$ ,  $\det S \in (\mathbf{Z}/k)^*$ . Равенства (1) можно переписать следующим образом:

$$\sum_{j=1}^n a_{ij} t_{jl} \equiv \sum_{j=1}^n t_{ij} a_{jl} \pmod{m}, \quad \sum_{j=1}^n a_{ij} s_{jl} \equiv \sum_{j=1}^n s_{ij} a_{jl} \pmod{k}, \quad i, l = 1, \dots, n. \quad (2)$$

Согласно китайской теореме об остатках

$$\mathbf{Z}/m \times \mathbf{Z}/k \cong \mathbf{Z}/mk. \quad (3)$$

Построим матрицу  $Q = (q_{ij})$ , элементы которой удовлетворяют условиям

$$\text{res}_m q_{ij} = t_{ij}, \quad \text{res}_k q_{ij} = s_{ij}. \quad (4)$$

Эта матрица строится однозначно в силу изоморфизма (3). Из (1), (2) и (4) вытекает, что

$$AQ \equiv AT \pmod{m}, \quad AQ \equiv AS \pmod{k}, \quad QB \equiv TB \pmod{m}, \quad QB \equiv SB \pmod{k}.$$

Следовательно,  $AQ \equiv QB \pmod{m}$  и  $AQ \equiv QB \pmod{k}$ , откуда  $AQ \equiv QB \pmod{mk}$  в силу взаимной простоты  $m$  и  $k$ .

Осталось доказать, что  $\det Q \in (\mathbf{Z}/mk)^*$ . Действительно,  $\text{res}_m(\det Q) = \text{res}_m(\det T) \in (\mathbf{Z}/m)^*$ ,  $\text{res}_k(\det Q) = \text{res}_k(\det S) \in (\mathbf{Z}/k)^*$ . Отсюда видно, что  $\det Q \in (\mathbf{Z}/mk)^*$ .  $\square$

**Следствие 1.** Если  $A \sim_{m_i} B$ , где  $i = 1, \dots, s$ ,  $\text{НОД}(m_i, m_j) = 1$  для всех  $i \neq j$ , то  $A \sim_q B$ , где  $q = m_1 \dots m_s$ .

**Следствие 2.** Если  $A \sim_q B$ , где  $q = p^k$  для любых простых  $p$  и натуральных  $k$ , то  $A \sim_m B$ , для любого натурального  $m \geq 2$ .

**Следствие 3.** Пусть  $A, B \in \mathbf{Z}^{n \times n}$  и существует матрица  $S \in \mathbf{Z}^{n \times n}$ , у которой  $\det S = p_1^{k_1} \dots p_s^{k_s}$  и  $AS = SB$ . Если  $A \sim_q B$  над  $\mathbf{Z}/q$ , где  $q = p_i^{k_i}$ ,  $i = 1, \dots, s$ , для любого натурального  $k$ , то  $A \sim_m B$  над  $\mathbf{Z}/m$  для всех  $m \geq 2$ .

**Доказательство.** Логически возможны два варианта.

1)  $\text{НОД}(m, \det S) = 1$ . Тогда  $AS \equiv SB \pmod{m}$ . Покажем, что  $\det S \in (\mathbf{Z}/m)^*$ . Действительно,  $\det S = p_1^{k_1} \cdots p_s^{k_s} \equiv r \pmod{m}$ , причем  $\text{НОД}(m, r) = 1$ , т. к. в противном случае имели бы противоречие с взаимной простотой  $m$  и  $\det S$ .

2)  $\text{НОД}(m, \det S) = d \neq 1$ . Таким образом,  $m = db$  и  $\text{НОД}(b, \det S) = 1$ . Тогда  $A \sim_d B$  по следствию 1 и  $A \sim_b B$  согласно предыдущему случаю. Следовательно, в силу взаимной простоты  $d$  и  $b$  и теоремы 2 получаем  $A \sim_m B$ .  $\square$

**Следствие 4.** Пусть  $A, B \in \mathbf{Z}^{n \times n}$  и существуют матрицы  $S_i \in \mathbf{Z}^{n \times n}$  такие, что  $AS_i = S_i B$ ,  $\det S_i \neq 0$ ,  $i = 1, \dots, l$ . Если  $\text{НОД}(\det S_1, \dots, \det S_l) = 1$ , то  $A \sim_m B$  для всех  $m \geq 2$ .

Пусть матрицы  $A$  и  $B$  имеют один и тот же характеристический многочлен  $d(\lambda)$ , который неприводим над  $\mathbf{Q}$ . Введем несколько обозначений:  $M_{A,B} = \{S \in \mathbf{Q}^{n \times n} \mid AS = SB\}$  и  $\Lambda_{A,B} = M_{A,B} \cap \mathbf{Z}^{n \times n}$ . Очевидно,  $M_{A,B}$  — подпространство в  $\mathbf{Q}^{n \times n}$ , а  $\Lambda_{A,B}$  — подмодуль в  $\mathbf{Z}^{n \times n}$ . В этом случае верно

**Утверждение** ([2], с. 193).  $M_{A,B} = L(S, AS, A^2S, \dots, A^{n-1}S) = L(S, SB, SB^2, \dots, SB^{n-1})$ , где  $S \in M_{A,B}$ ,  $\det S \neq 0$ , а буквой  $L$  обозначили множество всех линейных комбинаций матриц, стоящих в скобках.

Не уменьшая общности, можно считать, что  $S$  — целочисленная матрица. Пусть  $T_1, \dots, T_n$  — базис модуля  $\Lambda_{A,B}$ . Тогда очевидна

**Лемма 1.** Для того чтобы  $A \sim B$ , необходимо и достаточно, чтобы уравнение  $\det(x_1T_1 + \dots + x_nT_n) = \pm 1$  имело решение в целых  $x_1, \dots, x_n$ .

Если  $t_j^i$  есть  $j$ -й столбец матрицы  $T_i$ , то

$$f(x_1, \dots, x_n) = \det \left( \sum_{i=1}^n x_i T_i \right) = \sum_{i_1=1}^n \cdots \sum_{i_n=1}^n x_{i_1} \cdots x_{i_n} \det(t_1^{i_1}, \dots, t_n^{i_n}).$$

Нужно выяснить, имеет ли уравнение  $f(x_1, \dots, x_n) = \pm 1$  решение в целых числах. Как решать это уравнение в общем случае, неизвестно. Но если  $n = 2$ , то  $\det(x_1T_1 + x_2T_2) = x_1^2 \det T_1 + x_1x_2(\det(t_1^1, t_2^2) + \det(t_2^1, t_1^2)) + x_2^2 \det T_2$  — бинарная квадратичная форма, т. е. в этом случае задача о подобии сводится к классическому вопросу теории чисел — представлению целого числа (здесь  $\pm 1$ ) квадратичной формой (напр., [3], с. 286; [4], с. 310). Поэтому для более детального изучения перейдем к матрицам второго порядка. Из третьего необходимого условия подобия вытекает (при  $k = n$ ), что если  $A \sim B$ , то характеристические многочлены матриц совпадают. Будем это предполагать, не оговаривая специально.

## 1. Случай приводимого характеристического многочлена

Пусть  $\alpha \in \mathbf{Z}$  — корень многочлена  $d(\lambda)$  и  $x = (x_1, x_2)^T$  — собственный вектор, соответствующий  $\alpha$ . Не уменьшая общности, можно считать, что  $x \in \mathbf{Z}^2$  и  $\text{НОД}(x_1, x_2) = 1$ . Тогда существуют целые числа  $y_1, y_2$  такие, что  $\det \begin{pmatrix} x_1 & y_1 \\ x_2 & y_2 \end{pmatrix} = \det(x, y) = 1$ . Векторы  $x$  и  $y$  образуют базис в  $\mathbf{Q}^2$ . Разложим  $Ay$  по этому базису:  $Ay = c_1x + c_2y$ . В пространстве  $\mathbf{Q}^2$  определим линейное преобразование  $\varphi$  с матрицей  $A$ , т. е.  $[\varphi]_e = A$  в стандартном базисе  $e$ . Тогда в базисе  $x, y$

$$C = [\varphi]_{(x,y)} = \begin{pmatrix} \alpha & c_1 \\ 0 & c_2 \end{pmatrix}. \quad (5)$$

Таким образом,  $C = T^{-1}AT$ , где  $T = (x, y)$ . Следовательно,  $A \sim C$  и  $\text{tr } A = \text{tr } C$ ,  $\det A = \det C$  (где  $\text{tr } A$  — след матрицы, т. е. сумма элементов главной диагонали,  $\det A$  — определитель матрицы). Возможны два варианта:

- 1°.  $d(\lambda)$  имеет один двукратный корень,
- 2°.  $d(\lambda)$  имеет два различных корня.

1°. Имеем  $d(\lambda) = (\lambda - \alpha)^2 = \lambda^2 - 2\alpha\lambda + \alpha^2$ , т. е.  $\text{tr } A = 2\alpha$  и  $\det A = \alpha^2$ . Над полем рациональных чисел  $\mathbf{Q}$  имеем два класса  $Y_1(\alpha)$  и  $Y_2(\alpha)$  подобных матриц с каноническими матрицами  $R_0(\alpha) = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}$  и  $R_1(\alpha) = \begin{pmatrix} \alpha & 1 \\ 0 & \alpha \end{pmatrix}$  соответственно, т. е.  $Y_1(\alpha) = \{A \in \mathbf{Z}^{2 \times 2} \mid A \approx R_0(\alpha)\}$ ,  $Y_2(\alpha) = \{A \in \mathbf{Z}^{2 \times 2} \mid A \approx R_1(\alpha)\}$ . Посмотрим, что изменится над  $\mathbf{Z}$ . В силу вышесказанного  $c_2 = \alpha$ . Таким образом, выражение (5) принимает вид  $C = [\varphi]_{(x,y)} = \begin{pmatrix} \alpha & c_1 \\ 0 & \alpha \end{pmatrix}$ . Теперь заметим, что можно считать  $c_1 \geq 0$ , т. к. в противном случае, взяв  $T = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ , получим  $T^{-1}CT = \begin{pmatrix} \alpha & -c_1 \\ 0 & \alpha \end{pmatrix}$ . Из теоремы 1 следует, что матрицы  $R_{k_1}(\alpha) = \begin{pmatrix} \alpha & k_1 \\ 0 & \alpha \end{pmatrix}$  и  $R_{k_2}(\alpha) = \begin{pmatrix} \alpha & k_2 \\ 0 & \alpha \end{pmatrix}$ , где  $k_1, k_2 \geq 0$ , не подобны, если  $k_1 \neq k_2$ , т. к.  $I_1(R_1 - \lambda E) \neq I_1(R_2 - \lambda E)$ .

Матрицы  $R_{k_1}(\alpha)$  и  $R_{k_2}(\alpha)$  представляют разные классы эквивалентности и однозначно характеризуют класс, которому принадлежат. Поэтому матрица вида  $R_k(\alpha) = \begin{pmatrix} \alpha & k \\ 0 & \alpha \end{pmatrix}$ , где  $k \geq 0$ , является канонической. Таким образом, класс  $Y_2(\alpha)$  разбивается на счетное число подклассов  $K_j(\alpha) = \{A \in \mathbf{Z}^{2 \times 2} \mid A \sim R_j(\alpha)\}$ , каждый из которых характеризуется канонической матрицей  $R_j(\alpha) = \begin{pmatrix} \alpha & j \\ 0 & \alpha \end{pmatrix}$ , где  $j \geq 1$ . Тем самым доказана

**Теорема 3.** Если  $d(\lambda) = (\lambda - \alpha)^2$ , где  $\alpha \in \mathbf{Z}$ , то

- 1)  $A \sim B$  тогда и только тогда, когда  $I_1(A - \lambda E) = I_1(B - \lambda E)$ ,
- 2)  $Y_1(\alpha) = K_0(\alpha)$ ,  $Y_2(\alpha) = \bigcup_{j \geq 1} K_j(\alpha)$ , где  $K_j(\alpha) = \{A \in \mathbf{Z}^{2 \times 2} \mid A \sim R_j(\alpha)\}$ , а  $R_j(\alpha) = \begin{pmatrix} \alpha & j \\ 0 & \alpha \end{pmatrix}$ ,  $j \geq 0$ , — каноническая матрица.

2°. Если корни простые, то  $d(\lambda) = (\lambda - \alpha)(\lambda - \beta)$ , т. е.  $\text{tr } A = \alpha + \beta$  и  $\det A = \alpha\beta$ . Не уменьшая общности, можно считать, что  $\beta > \alpha$ . Над полем  $\mathbf{Q}$  имеем один класс  $Y_3(\alpha, \beta) = \{A \in \mathbf{Z}^{2 \times 2} \mid A \approx R_0(\alpha, \beta)\}$  подобных матриц с канонической матрицей  $R_0(\alpha, \beta) = \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}$ . Найдется собственный вектор  $x = (x_1, x_2)^T \in \mathbf{Z}^2$  с НОД( $x_1, x_2$ ) = 1, соответствующий  $\alpha$ , т. е.  $Ax = \alpha x$ . Найдем  $y = (y_1, y_2)^T \in \mathbf{Z}^2$  такой, что  $\det(x, y) = 1$ . В данном случае  $c_2 = \beta$ . Тогда (5) примет вид  $C = [\varphi]_{(x,y)} = \begin{pmatrix} \alpha & c_1 \\ 0 & \beta \end{pmatrix}$ . Во-первых, можно считать, что  $0 \leq c_1 < \beta - \alpha$ . Действительно,  $c_1 = q(\beta - \alpha) + r$ , где  $0 \leq r < \beta - \alpha$ . Тогда  $T^{-1}CT = \begin{pmatrix} \alpha & r \\ 0 & \beta \end{pmatrix} = R_r(\alpha, \beta)$ , если  $T = \begin{pmatrix} 1 & q \\ 0 & 1 \end{pmatrix}$ . Во-вторых, можно считать, что  $0 \leq c_1 \leq \lfloor \frac{\beta - \alpha}{2} \rfloor$ , т. к.  $S^{-1}R_r(\alpha, \beta)S = \begin{pmatrix} \alpha & (\beta - \alpha) - r \\ 0 & \beta \end{pmatrix}$ , где  $S = \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix}$ . Теперь убедимся в том, что матрицы  $R_{k_1}(\alpha, \beta) = \begin{pmatrix} \alpha & k_1 \\ 0 & \beta \end{pmatrix}$  и  $R_{k_2}(\alpha, \beta) = \begin{pmatrix} \alpha & k_2 \\ 0 & \beta \end{pmatrix}$  не подобны, если  $k_1 \neq k_2$  и  $0 \leq k_1, k_2 \leq \lfloor \frac{\beta - \alpha}{2} \rfloor$ . Предположим, что найдется унимодулярная матрица  $T = \begin{pmatrix} t_{11} & t_{12} \\ t_{21} & t_{22} \end{pmatrix}$  такая, что  $R_{k_1}(\alpha, \beta)T = TR_{k_2}(\alpha, \beta)$ . Тогда  $R_{k_1}(\alpha, \beta)T = \begin{pmatrix} \alpha t_{11} + k_1 t_{21} & \alpha t_{12} + k_1 t_{22} \\ \beta t_{21} & \beta t_{22} \end{pmatrix} = \begin{pmatrix} \alpha t_{11} & k_2 t_{11} + \beta t_{12} \\ \alpha t_{21} & k_2 t_{21} + \beta t_{22} \end{pmatrix} = TR_{k_2}(\alpha, \beta)$ . Отсюда видим, что  $t_{21} = 0$  и  $(\beta - \alpha)t_{12} = k_1 t_{22} - k_2 t_{11}$ , значит,  $t_{11} t_{22} = \pm 1$  и  $(\beta - \alpha)t_{12} = \pm k_1 \pm k_2$ . Но тогда  $t_{12}$  не может быть целым в силу ограничений на  $k_1, k_2$ . Таким образом, над кольцом  $\mathbf{Z}$  класс  $Y_3(\alpha, \beta)$  разделился на конечное число подклассов  $K_j(\alpha, \beta) = \{A \in \mathbf{Z}^{2 \times 2} \mid A \sim R_j(\alpha, \beta)\}$ , и матрица вида  $R_j(\alpha, \beta) = \begin{pmatrix} \alpha & j \\ 0 & \beta \end{pmatrix}$ , где  $0 \leq j \leq \lfloor \frac{\beta - \alpha}{2} \rfloor$ , является канонической. Из вышеизложенного следует

**Теорема 4.** Если  $d(\lambda) = (\lambda - \alpha)(\lambda - \beta)$ ,  $\alpha, \beta \in \mathbf{Z}$ ,  $\beta > \alpha$ , то  $Y_3(\alpha, \beta) = \bigcup_{j=0}^{\lfloor \frac{\beta - \alpha}{2} \rfloor} K_j(\alpha, \beta)$ , где  $K_j(\alpha, \beta) = \{A \in \mathbf{Z}^{2 \times 2} \mid A \sim R_j(\alpha, \beta)\}$ , а  $R_j(\alpha, \beta) = \begin{pmatrix} \alpha & j \\ 0 & \beta \end{pmatrix}$ ,  $0 \leq j \leq \lfloor \frac{\beta - \alpha}{2} \rfloor$ , — каноническая матрица.

Теорема 4 позволяет строить примеры, показывающие, что условия, сформулированные в теореме 1, не являются достаточными для подобия двух матриц.

**Пример 1.** Рассмотрим  $A = \begin{pmatrix} 1 & 1 \\ 0 & 6 \end{pmatrix}$  и  $B = \begin{pmatrix} 1 & 2 \\ 0 & 6 \end{pmatrix}$ . Выполнение первого, третьего и четвертого условий очевидно, причем  $AT = TB$ , где  $T = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ . Для проверки второго условия в силу следствия 3 достаточно показать, что  $A \sim_m B$ , где  $m = 2^k$ ,  $k$  — натуральное число. Для этого в качестве трансформирующей матрицы можно взять  $S = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ . Но по теореме 4  $A$  и  $B$  — канонические матрицы из разных классов эквивалентности, т. е. они не подобны.

Пусть  $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ ,  $B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$ . Следовательно,  $t = a_{11} + a_{22} = b_{11} + b_{22}$ ,  $s = \det A = \det B$ , а характеристический многочлен имеет вид  $d(\lambda) = \lambda^2 - t\lambda + s$ . Очевидно, если  $\alpha \in \mathbf{Z}$ , то  $A$  и  $B$

подобны над  $\mathbf{Z}$  тогда и только тогда, когда  $A - \alpha E$  и  $B - \alpha E$  подобны над  $\mathbf{Z}$ . Если в качестве  $\alpha$  взять  $[\frac{t}{2}]$ , то возможны два случая.

1)  $t$  — четное число. Тогда след матриц  $A - \alpha E$  и  $B - \alpha E$  будет равен 0, а характеристический многочлен запишется в виде

$$d(\lambda) = \lambda^2 - d, \quad (6)$$

где  $d = \alpha^2 - \det A$ . В этом случае

$$A - \alpha E = \begin{pmatrix} a & a_1 \\ a_2 & -a \end{pmatrix}, \quad B - \alpha E = \begin{pmatrix} b & b_1 \\ b_2 & -b \end{pmatrix}. \quad (7)$$

2)  $t$  — нечетное число. Тогда след матриц  $A - \alpha E$  и  $B - \alpha E$  будет равен 1, а характеристический многочлен

$$d(\lambda) = \lambda^2 - \lambda - d, \quad (8)$$

где  $d = \alpha^2 + \alpha - \det A$ . В этом случае

$$A - \alpha E = \begin{pmatrix} a + 1 & a_1 \\ a_2 & -a \end{pmatrix}, \quad B - \alpha E = \begin{pmatrix} b + 1 & b_1 \\ b_2 & -b \end{pmatrix}. \quad (9)$$

Итак, исходную задачу свели к задаче о подобии матриц вида (7) или (9).

## 2. Случай неприводимого характеристического многочлена

Итак, предполагаем, что характеристический многочлен (имеющий вид (6) или (8)) неприводим над полем  $\mathbf{Q}$  (отсюда, в частности, следует, что  $A$  и  $B$  невырождены).

Рассмотрим сначала случай, когда  $d(\lambda) = \lambda^2 - \lambda - d$ . В этом случае  $A = \begin{pmatrix} a+1 & a_1 \\ a_2 & -a \end{pmatrix}$  подобна над полем рациональных чисел матрице Фробениуса  $F = \begin{pmatrix} 1 & 1 \\ d & 0 \end{pmatrix}$ , где  $d = a^2 + a + bc$ ,  $b \neq 0$  и  $c \neq 0$ . Это следует из того, что НОД миноров любого порядка их характеристических матриц одинаковы (действительно, НОД миноров первого порядка равен 1, а второго —  $d(\lambda)$ ). Выясним, останется ли этот факт верным над  $\mathbf{Z}$ . Базисом модуля  $\Lambda_{A,F}$  являются матрицы  $\begin{pmatrix} a+1 & 1 \\ c & 0 \end{pmatrix}$  и  $\begin{pmatrix} b & 0 \\ -a & 1 \end{pmatrix}$ . Таким образом,  $\Lambda_{A,F}$  состоит из матриц вида  $S = \begin{pmatrix} x(a+1)+y & x \\ cx-ay & y \end{pmatrix}$ ,  $x, y \in \mathbf{Z}$ , а  $\det S = -cx^2 + (2a+1)xy + by^2$ . Получили бинарную квадратичную форму. Заметим, что ее дискриминант совпадает с дискриминантом исходного характеристического многочлена. Выясним, разрешимо ли в целых числах уравнение

$$-cx^2 + (2a+1)xy + by^2 = \pm 1. \quad (10)$$

Домножив (10) на  $4b$ , получим равносильное (10) уравнение

$$(2by + (2a+1)x)^2 - Dy^2 = \pm 4b, \quad (11)$$

где  $D = 1 + 4d$ . Для того чтобы уравнение (11) имело решение в целых  $x$  и  $y$  (а, соответственно, и для подобия матриц  $A$  и  $F$ ), необходимо, чтобы для любого простого  $p$ , являющегося делителем  $D$ , хотя бы одно из чисел  $\pm 4b$  было полным квадратом в поле вычетов  $\mathbf{Z}/p$ . Тем самым получили пятое необходимое условие подобия при  $p \equiv 1 \pmod{4}$ , т. к. в противном случае (если  $p \equiv -1 \pmod{4}$ ) либо  $4b$ , либо  $-4b$  является полным квадратом в  $\mathbf{Z}/p$ . Заметим, что в силу равноправия  $b$  и  $c$  аналогичное необходимое условие формулируется и для  $c$ .

Теперь перейдем к случаю, когда  $d(\lambda) = \lambda^2 - d$ . При этом  $A = \begin{pmatrix} a & b \\ c & -a \end{pmatrix}$  подобна над полем  $\mathbf{Q}$  матрице Фробениуса  $F = \begin{pmatrix} 0 & 1 \\ d & 0 \end{pmatrix}$ , где  $d = a^2 + bc$ ,  $b \neq 0$  и  $c \neq 0$ . Здесь базисом модуля  $\Lambda_{A,F}$  являются матрицы  $\begin{pmatrix} a & 1 \\ c & 0 \end{pmatrix}$  и  $\begin{pmatrix} b & 0 \\ -a & 1 \end{pmatrix}$ , т. е. любая матрица из  $\Lambda_{A,F}$  имеет вид  $S = \begin{pmatrix} ax+by & x \\ cx-ay & y \end{pmatrix}$ ,  $x, y \in \mathbf{Z}$ , а  $\det S = -cx^2 + 2axy + by^2$ . Аналогично предыдущему случаю имеем уравнение  $-cx^2 + 2axy + by^2 = \pm 1$ , эквивалентное

$$(by + ax)^2 - dy^2 = \pm b. \quad (12)$$

Чтобы (12) имело решение в целых числах, получаем аналогичное предыдущему случаю необходимое условие (хотя бы одно из чисел  $\pm b$  и хотя бы одно из чисел  $\pm c$  должны быть полными квадратами в поле вычетов  $\mathbf{Z}/p$  для любого простого  $p$ , являющегося делителем  $d$ ).

Пятое необходимое условие не следует из первых четырех, что показывает

**Пример 2.**  $A = \begin{pmatrix} 0 & 2 \\ 5 & 0 \end{pmatrix}$ ,  $F = \begin{pmatrix} 0 & 1 \\ 10 & 0 \end{pmatrix}$ ,  $d = 10$ ;  $A \approx F$ , т. к.  $AS = SF$ , где  $S = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$ . Для проверки второго необходимого условия в силу следствия 3 достаточно убедиться, что  $A \sim_m F$  для  $m = 2^k$ . Здесь в качестве трансформирующей можно взять матрицу  $T = \begin{pmatrix} 0 & 1 \\ 5 & 0 \end{pmatrix}$ . Но пятое необходимое условие нарушается, т. к. ни одно из чисел  $\pm 2$  не является квадратом в поле вычетов  $\mathbf{Z}/5$ . Следовательно,  $A$  и  $F$  не подобны над  $\mathbf{Z}$ .

Это еще один пример, показывающий, что необходимые условия подобия, сформулированные в теореме 1, не являются достаточными. Но и все пять необходимых условий в совокупности не являются достаточными. Это мы продемонстрируем на следующем примере (который получен на основе примера из ([4], с. 314)).

**Пример 3.** Рассмотрим  $A = \begin{pmatrix} 0 & 2 \\ 41 & 0 \end{pmatrix}$ ,  $F = \begin{pmatrix} 0 & 1 \\ 82 & 0 \end{pmatrix}$ ,  $d = 82$ . Нетрудно проверить выполнение необходимых условий из теоремы 1. Справедливость пятого условия следует из того, что оба числа  $\pm 2$  являются квадратами в поле вычетов  $\mathbf{Z}/41$ , а именно,  $11^2 \equiv -2 \pmod{41}$  и  $17^2 \equiv 2 \pmod{41}$ . Но, несмотря на это, квадратичная форма  $2y^2 - 41x^2$  не представляет ни одно из чисел  $\pm 1$ , т. е.  $A$  и  $F$  не подобны над  $\mathbf{Z}$ .

**Теорема 5.** Если  $d(\lambda)$  неприводим над  $\mathbf{Q}$ , то множество матриц с характеристическим многочленом  $d(\lambda)$  распадается на конечное число классов эквивалентности.

**Доказательство.** 1) Пусть  $d > 0$ . Рассмотрим случай, когда  $d(\lambda) = \lambda^2 - d$ . Тогда  $A = \begin{pmatrix} a & b \\ c & -a \end{pmatrix}$ ,  $a \geq 0$ ,  $a^2 + bc = d > 0$ . Докажем, что существует такое  $r \geq 0$ , что  $A \sim \begin{pmatrix} r & b_1 \\ c_1 & -r \end{pmatrix}$ , где

$$b_1 \geq r + 1, \quad c_1 \geq r + 1. \quad (13)$$

Не уменьшая общности, можно считать, что  $b > 0$  или  $c > 0$ . Действительно, если  $b < 0$ , то  $A \sim B$ , где  $B = \begin{pmatrix} a & -b \\ -c & -a \end{pmatrix}$ , т. к.  $AE_1 = E_1B$ , а  $E_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$  (аналогично, если  $c < 0$ ).

Заметим, что если  $|b| \geq a + 1$  и  $|c| \geq a + 1$ , то  $bc > 0$ , т. к. в противном случае имели бы  $a^2 > -bc \geq (a + 1)^2$ , что неверно. С учетом предыдущего замечания в этом случае можно считать, что  $b > 0$  и  $c > 0$ .

Возможны три варианта.

1. Если  $0 < b \leq a$ , то, разделив  $a$  на  $b$  с остатком, получим  $a = q_1b + r_1$ , где  $0 \leq r_1 < b$ . Тогда  $AT = TB_1$ , где  $T = \begin{pmatrix} 1 & 0 \\ -q_1 & 1 \end{pmatrix}$ , а  $B_1 = \begin{pmatrix} r_1 & b \\ c_1 & -r_1 \end{pmatrix}$ .

2. Если  $0 < c \leq a$ , то, разделив  $a$  на  $c$  с остатком, получим  $a = q_2c + r_2$ , где  $0 \leq r_2 < c$ . Тогда  $AS = SB_2$ , где  $S = \begin{pmatrix} 1 & q_2 \\ 0 & 1 \end{pmatrix}$ , а  $B_2 = \begin{pmatrix} r_2 & b_2 \\ c & -r_2 \end{pmatrix}$ .

3. Если  $b \geq a + 1$  и  $c \geq a + 1$ , то условия (13) выполнены, что и требовалось.

После выполнения действий в первом или во втором вариантах для новой матрицы ( $B_1$  или  $B_2$ ) снова будет справедлив один из трех вариантов. Но с каждым шагом элемент  $a$  на главной диагонали будет уменьшаться и в силу его неотрицательности в конце концов придем к третьему варианту. Тогда  $d = a^2 + bc \geq a^2 + (a + 1)^2$ , откуда следует  $a \leq \lfloor \frac{\sqrt{2d-1}-1}{2} \rfloor$ .

Аналогично рассматривается случай, когда  $d(\lambda) = \lambda^2 - \lambda - d$ . При этом ограничение на  $a$  имеет вид  $a \leq \lfloor \frac{\sqrt{8d+1}-3}{4} \rfloor$ .

2) Пусть  $d < 0$ . Здесь можно применить те же действия, которые проводились в предыдущем случае, и добиться того, чтобы для матрицы  $A = \begin{pmatrix} a & b \\ c & -a \end{pmatrix}$ ,  $a \geq 0$ ,  $a^2 + bc = d < 0$ , имели место неравенства  $b \geq a + 1$ ,  $c \geq a + 1$ . В этом случае  $-d = |d| = -bc - a^2 \geq (a + 1)^2 - a^2 = 2a + 1$ , откуда  $a \leq \lfloor \frac{|d|-1}{2} \rfloor$ . Если же  $d(\lambda) = \lambda^2 - \lambda - d$ , то  $|d| = -bc - a^2 - a \geq (a + 1)^2 - a^2 - a = a + 1$ , откуда  $a \leq \lfloor |d| - 1 \rfloor$ .  $\square$

Пусть  $S_1$  и  $S_2$  — базис  $\Lambda_{A,B}$ , тогда произвольную матрицу из  $\Lambda_{A,B}$  можно представить в виде  $xS_1 + yS_2$  для некоторых  $x$  и  $y$  из  $\mathbf{Z}$ . Наша задача состоит в том, чтобы определить, существует ли в  $\Lambda_{A,B}$  матрица с определителем 1 или  $-1$ . Пусть  $S \in \Lambda_{A,B}$ , тогда  $\det S = f(x, y) = \det(xS_1 + yS_2) = x^2 \det S_1 + xy(\det(s_1^1, s_2^1) + \det(s_1^2, s_2^1)) + y^2 \det S_2$ , где  $s_1^1, s_2^1$  — столбцы матрицы  $S_1$ , а  $s_1^2, s_2^2$  — столбцы матрицы  $S_2$ .

**Теорема 6.** Пусть  $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ ,  $B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$  и их характеристический многочлен  $d(\lambda)$  неприводим над  $\mathbf{Q}$ . Тогда базис модуля  $\Lambda_{A,B}$  образуют матрицы  $T_1 = \frac{1}{\delta_1} \begin{pmatrix} a_{12} & 0 \\ b_{11}-a_{11} & b_{12} \end{pmatrix}$  и  $T_2 = \frac{1}{\Delta} \begin{pmatrix} \frac{a_{12}}{\delta_2} \gamma & \frac{a_{12}}{\delta_2} \\ \frac{b_{21} + \frac{b_{11}-a_{11}}{\delta_1} \gamma}{\delta_2} & \frac{b_{22}-a_{11} + \frac{b_{12}}{\delta_1} \gamma}{\delta_2} \end{pmatrix}$ , где  $\delta_1 = \text{НОД}(a_{12}, b_{12}, b_{11} - a_{11})$ ,  $\delta_2 = \text{НОД}(a_{12}, b_{21}, b_{22} - a_{11})$ ,  $\Delta = \text{НОД}(\frac{a_{12}}{\delta_1}, \frac{a_{12}}{\delta_2})$ , а  $\gamma$  удовлетворяет сравнению  $\frac{b_{12}}{\delta_1} \gamma \equiv \frac{a_{11}-b_{22}}{\delta_2} \pmod{\Delta}$ .

**Доказательство.** Так как  $d(\lambda)$  неприводим, то  $a_{12} \neq 0$ . Прежние обозначения при  $n = 2$  имеют вид  $M_{A,B} = \{S \in \mathbf{Q}^{2 \times 2} \mid AS = SB\}$  и  $\Lambda_{A,B} = M_{A,B} \cap \mathbf{Z}^{2 \times 2}$ . В качестве базиса  $M_{A,B}$  можно взять матрицы  $S_1 = \begin{pmatrix} a_{12} & 0 \\ b_{11}-a_{11} & b_{12} \end{pmatrix}$ ,  $S_2 = \begin{pmatrix} 0 & a_{12} \\ b_{21} & b_{22}-a_{11} \end{pmatrix}$ .

Обозначим  $\delta_1 = \text{НОД}(a_{12}, b_{12}, b_{11} - a_{11})$ ,  $\delta_2 = \text{НОД}(a_{12}, b_{21}, b_{22} - a_{11})$ . Следовательно,  $S_1$  и  $S_2$  можно сократить на  $\delta_1$  и  $\delta_2$  соответственно. Получим матрицы  $S'_1, S'_2$ . Их можно представить в виде четырехмерных векторов  $s_1 = (\frac{a_{12}}{\delta_1} 0 \frac{b_{11}-a_{11}}{\delta_1} \frac{b_{12}}{\delta_1})^T$ ,  $s_2 = (0 \frac{a_{12}}{\delta_2} \frac{b_{21}}{\delta_2} \frac{b_{22}-a_{11}}{\delta_2})^T$ , образующих матрицу  $G = \begin{pmatrix} \frac{a_{12}}{\delta_1} & 0 & \frac{b_{11}-a_{11}}{\delta_1} & \frac{b_{12}}{\delta_1} \\ 0 & \frac{a_{12}}{\delta_2} & \frac{b_{21}}{\delta_2} & \frac{b_{22}-a_{11}}{\delta_2} \end{pmatrix}^T$ . Очевидно, подпространство  $L$  в  $\mathbf{Q}^4$ , базис которого образуют  $s_1, s_2$ , изоморфно  $M_{A,B}$ . Нам нужно найти базис модуля  $L \cap \mathbf{Z}^4$ . НОД элементов матрицы  $G$  равен 1, а НОД миноров второго порядка равен

$$\begin{aligned} \Delta &= \text{НОД}\left(\frac{a_{12}a_{12}}{\delta_1\delta_2}, \frac{a_{12}b_{21}}{\delta_1\delta_2}, \frac{a_{12}(b_{22}-a_{11})}{\delta_1\delta_2}, \frac{a_{12}b_{12}}{\delta_1\delta_2}, \frac{a_{12}(b_{11}-a_{11})}{\delta_1\delta_2}, \frac{a_{12}a_{21}}{\delta_1\delta_2}\right) = \\ &= \text{НОД}\left(\frac{a_{12}}{\delta_1} \text{НОД}\left(\frac{a_{12}}{\delta_2}, \frac{b_{21}}{\delta_2}, \frac{b_{22}-a_{11}}{\delta_2}\right), \frac{a_{12}}{\delta_2} \text{НОД}\left(\frac{b_{12}}{\delta_1}, \frac{b_{11}-a_{11}}{\delta_1}, \frac{a_{21}}{\delta_1}\right)\right) = \text{НОД}\left(\frac{a_{12}}{\delta_1}, \frac{a_{12}}{\delta_2}\right). \end{aligned}$$

Рассмотрим систему сравнений  $G \begin{pmatrix} x \\ y \end{pmatrix} \equiv 0 \pmod{\Delta}$ , которая эквивалентна одному сравнению

$$\frac{b_{12}}{\delta_1}x + \frac{b_{22}-a_{11}}{\delta_2}y \equiv 0 \pmod{\Delta}.$$

Множество решений данного сравнения является аддитивной циклической группой. Пусть  $(\alpha, \beta)$  — ее порождающий элемент, тогда  $\alpha s_1 + \beta s_2 \equiv 0 \pmod{\Delta}$ , причем  $\text{НОД}(\beta, \Delta) = \text{НОД}(\alpha, \Delta) = 1$ , т. к. в противном случае хотя бы один из векторов  $s_1, s_2$  можно было бы сократить на некоторый множитель. Следовательно, в качестве порождающего можно взять вектор  $(\gamma, 1)$ , где  $\gamma$  удовлетворяет сравнению  $\frac{b_{12}}{\delta_1} \gamma \equiv \frac{a_{11}-b_{22}}{\delta_2} \pmod{\Delta}$ . Таким образом, базис модуля  $L \cap \mathbf{Z}^4$  образуют векторы  $s_1$  и  $s_3 = \frac{1}{\Delta}(\gamma s_1 + s_2) = \frac{1}{\Delta} \left( \frac{a_{12}}{\delta_1} \gamma \frac{a_{12}}{\delta_2} \frac{b_{21} + \frac{b_{11}-a_{11}}{\delta_1} \gamma}{\delta_2} \frac{b_{22}-a_{11} + \frac{b_{12}}{\delta_1} \gamma}{\delta_2} \right)^T$ . Значит, базис модуля  $\Lambda_{A,B}$  образуют матрицы  $T_1 = S'_1 = \frac{1}{\delta_1} \begin{pmatrix} a_{12} & 0 \\ b_{11}-a_{11} & b_{12} \end{pmatrix}$  и  $T_2 = \frac{1}{\Delta}(\gamma S'_1 + S'_2) = \frac{1}{\Delta} \begin{pmatrix} \frac{a_{12}}{\delta_1} \gamma & \frac{a_{12}}{\delta_2} \\ \frac{b_{21} + \frac{b_{11}-a_{11}}{\delta_1} \gamma}{\delta_2} & \frac{b_{22}-a_{11} + \frac{b_{12}}{\delta_1} \gamma}{\delta_2} \end{pmatrix}$ .  $\square$

**Следствие 5.** Пусть верны условия предыдущей теоремы. Тогда квадратичная форма  $f(x, y)$  имеет вид  $f(x, y) = x^2 \frac{a_{12}b_{12}}{\delta_1^2} + xy \left( 2 \frac{a_{12}b_{12}}{\delta_1^2} \gamma + \frac{a_{12}(b_{22}-b_{11})}{\delta_1\delta_2\Delta} \right) + y^2 \left( \frac{a_{12}b_{12}}{\delta_1^2\Delta^2} \gamma^2 + \frac{a_{12}(b_{22}-b_{11})}{\delta_1\delta_2\Delta^2} - \frac{a_{12}b_{21}}{\delta_2^2\Delta^2} \right)$  и  $\frac{d}{D} = (\delta_1, \delta_2)^2$ , где  $d$  — дискриминант  $d(\lambda)$ ,  $D$  — дискриминант  $f(x, y)$ ,  $(\delta_1, \delta_2)$  — НОД  $\delta_1$  и  $\delta_2$ .

### 3. Алгоритм определения подобия

Даны две матрицы  $A, B \in \mathbf{Z}^{2 \times 2}$

1. Находим  $\text{tr } A$  и  $\text{tr } B$ . Если  $\text{tr } A \neq \text{tr } B$ , то  $A$  и  $B$  не подобны. Если  $\text{tr } A = \text{tr } B$ , то переходим к п. 2.

2. Находим  $\det A$  и  $\det B$ . Если  $\det A \neq \det B$ , то  $A$  и  $B$  не подобны. Если  $\det A = \det B$ , то переходим к п. 3.

3. Пусть  $d(\lambda) = \lambda^2 - a\lambda + b$  — характеристический многочлен матриц  $A$  и  $B$ , где  $a = \text{tr } A = \text{tr } B$ ,  $b = \det A = \det B$ . Если  $d(\lambda)$  приводим над  $\mathbf{Z}$ , т. е. имеет вид  $d(\lambda) = (\lambda - \alpha)(\lambda - \beta)$ ,  $\alpha, \beta \in \mathbf{Z}$ , то переходим к п. 4, в противном случае к п. 5.

4. Находим векторы  $x^A, x^B \in \mathbf{Z}^2$  — собственные векторы матриц  $A$  и  $B$ , соответствующие  $\alpha$ , такие, что  $\text{НОД}(x_1^A, x_2^A) = 1$ ,  $\text{НОД}(x_1^B, x_2^B) = 1$ . Находим такие векторы  $y^A, y^B \in \mathbf{Z}^2$ , что  $\det(x^A, y^A) = 1$ ,  $\det(x^B, y^B) = 1$ . Далее раскладываем вектор  $Ay^A$  по базису  $x^A, y^A$ , а вектор  $Bx^B$  по базису  $x^B, y^B$ . Получаем  $Ay^A = c_1x^A + \beta y^A$ ,  $Bx^B = c_2x^B + \beta y^B$ . Обозначим  $S_1 = (x^A, y^A)$ ,  $S_2 = (x^B, y^B)$ . Если  $\alpha = \beta$ , то переходим к п. 4.1, иначе к п. 4.2.

4.1. Если  $c_1 = c_2$ , то  $A \sim B$  и  $AS = SB$ , где  $S = S_1S_2^{-1}$ . Если  $c_1 = -c_2$ , то  $A \sim B$  и  $AS = SB$ , где  $S = S_1T^{-1}S_2^{-1}$ ,  $T = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ . Если  $|c_1| \neq |c_2|$ , то  $A$  и  $B$  не подобны.

4.2. Считаем, что  $\beta > \alpha$ . Делим с остатком  $c_1$  и  $c_2$  на  $\beta - \alpha$ . Получаем  $c_1 = q_1(\beta - \alpha) + r_1$ ,  $c_2 = q_2(\beta - \alpha) + r_2$ . Если  $r_1 = r_2$ , то  $A \sim B$  и  $AS = SB$ , где  $S = S_1T_1T_2^{-1}S_2^{-1}$ ,  $T_1 = \begin{pmatrix} 1 & q_1 \\ 0 & 1 \end{pmatrix}$ ,  $T_2 = \begin{pmatrix} 1 & q_2 \\ 0 & 1 \end{pmatrix}$ . Если  $r_1 = \beta - \alpha - r_2$ , то  $A \sim B$  и  $AS = SB$ , где  $S = S_1T_1QT_2^{-1}S_2^{-1}$ ,  $Q = \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix}$ . В противном случае  $A$  и  $B$  не подобны.

5. Находим квадратичную форму  $f(x, y)$ , фигурирующую в следствии 5, и ее дискриминант  $D$ . Если  $D < 0$ , то переходим к п. 5.1, если  $D > 0$ , то к п. 5.2.

5.1.  $f(x, y)$  — положительно определенная форма. Для выяснения вопроса о представимости целого числа этой формой применяется алгоритм приведения Гаусса (напр., [3], с. 293–294).

5.2.  $f(x, y)$  — неопределенная форма. В этом случае можно применить алгоритм из [5].

*Трудоёмкость алгоритма.* На вход алгоритма подаются две целочисленные матрицы  $A$  и  $B$ . Будем считать, что элементы этих матриц ограничены по модулю константой  $C$ . Пусть  $n = \log C$  — длина представления числа  $C$ . Очевидно, алгоритм, приведенный выше, является полиномиальным относительно  $n$ , если  $d(\lambda)$  приводим. Алгоритм приведения Гаусса также является полиномиальным. Алгоритм из [5] не полиномиален, т. к. он использует разложение квадратичной иррациональности  $\frac{P_0 + \sqrt{D}}{Q_0}$  в цепную дробь, которая является периодической с длиной периода  $l = O(\sqrt{D} \log D)$ . Вопрос о существовании полиномиального решающего алгоритма в случае, если  $f(x, y)$  — неопределенная форма, остается открытым.

Часть результатов, представленная в данной статье, была анонсирована в ([6], с. 112).

## Литература

1. Мальцев А.И. *Основы линейной алгебры*. — М.—Л.: Гостехиздат, 1948. — 424 с.
2. Гантмахер Ф.Р. *Теория матриц*. — М.: Наука, 1988. — 552 с.
3. Бухштаб А.А. *Теория чисел*. — М.: Просвещение, 1966. — 384 с.
4. Касселс Дж. *Рациональные квадратичные формы*. — М.: Мир, 1982. — 440 с.
5. Matthews К. *The diophantine equation  $ax^2 + bxy + cy^2 = N$ ,  $D = b^2 - 4ac > 0$*  // J. Theor. Nombres Bordeaux. — 2002. — V. 14. — P. 257–270.
6. Шевченко В.Н., Сидоров С.В. *О подобии матриц второго порядка над кольцом целых чисел* // Материалы XIV Международн. школы-семинара “Синтез и сложность управляющих систем” (Нижний Новгород, 27 октября–1 ноября 2003 г.) / Под ред. О.Б. Лупанова. — Н. Новгород: Изд-во. Нижегородск. гос. пед. ун-та, 2003. — 131 с.

Нижегородский государственный  
университет

Поступила  
30.09.2004